Configuring Prime Cable Provisioning Using Admin UI

This chapter describes the Prime Cable Provisioning configuration tasks that you perform by selecting the options in the Configuration menu:

Configuring Class of Service

Using the Prime Cable Provisioning Admin UI, you can configure the Class of Service offered to your customers. For example, you can associate DOCSIS options with different DOCSIS Class of Service. You use the Prime Cable Provisioning Admin UI to add, modify, or delete any selected Class of Service.

To configure Class of Service, click **Configuration** > **Class of Service**.

Adding a Class of Service

To add a Class of Service:

Step 1 From the Manage Class of Service page, select the device type from the Class of Service drop-down list.

Step 2 Click **Add**.

Step 3 Enter the name for the new Class of Service.

Step 4 If you want to change the Class of Service, choose it from the Type drop-down list. For example, assume that you want to create a new Class of Service called Gold-Classic for DOCSIS modems. You might enter Gold-Classic as the Class of Service Name, and choose DOCSISModem from the service type drop-down list.

Step 5 Click **Assign Domain** and select the domain to which the property must belong. Click **Apply** to save the changes.

Note The options related to domain management and domain assignment are not enabled by default. For details, see Adding a Domain.

Step 6 Click **Add Property** and choose a property and enter its corresponding value in the Property Value field. For example, if you choose the property name */cos/docsis/file,* enter Gold-Classic.cm in the Property Value field, and continue with the rest of this procedure.

Note When adding a DOCSIS Modem Class of Service, you must specify the */cos/docsis/file* property with the value being the name of a previously added file. This file is used when provisioning a DOCSIS device that has this Class of Service. Prime Cable Provisioning provides automatic selection of a cable modem configuration file that enables the highest DOCSIS version compatible with the modem. To enable this feature, you must configure the Class of Service with multiple configuration files, one for each DOCSIS level. Use the following properties to allow the selection of a configuration file specific to a DOCSIS version:

- */cos/docsis/file/1.0*—Selects a configuration file specific to DOCSIS 1.0.
- */cos/docsis/file/1.1*—Selects a configuration file specific to DOCSIS 1.1.
- */cos/docsis/file/2.0*—Selects a configuration file specific to DOCSIS 2.0.
- */cos/docsis/file/3.0*—Selects a configuration file specific to DOCSIS 3.0.
- */cos/docsis/file/3.1*—Selects a configuration file specific to DOCSIS 3.1.
- */cos/docsis/file/3.1/ipv4*—Selects a configuration file specific to DOCSIS 3.1 in the IPv4 mode.
- */cos/docsis/file/3.1/ipv6*—Selects a configuration file specific to DOCSIS 3.1 in the IPv6 mode.

When adding a PacketCable Class of Service, you must specify the */cos/packetCableMTA/file* property with the value being the name of a previously added file. This file is used when provisioning a PacketCable device that has this Class of Service.

When adding a CableHome WAN-MAN Class of Service, you must specify the */cos/cableHomeWanMan/file* property with the value being the name of a previously added file. This file is used when provisioning a CableHome WAN-MAN device that has this Class of Service.

Step 7 Click **Save** to add the property to the Class of Service.

Step 8 Click **Submit** to finalize the process.

After submitting the Class of Service, the Manage Class of Service page appears to show the newly added Class of Service for the particular device type.

Modifying a Class of Service

You modify your Class of Service by selecting the various properties and assigning appropriate property values. When creating a Class of Service for the first time you must select all the required properties and assign values to them. If you make a mistake, or your business requirements for a certain Class of Service change, you can either change the property value before submitting your previous changes or delete the Property Name:Property Value pair altogether.

Note Changes to the Class of Service object trigger the Configuration Regeneration Service (CRS) to regenerate configurations for all affected devices and send configurations to the DPEs. The CRS performs this task as a background job.

You can view the status of the CRS from the View RDU Details page.

To modify Class of Service properties, select the Class of Service for the specific device type. Make the necessary changes and click Submit.

Each property added to a Class of Service appears when you click **Submit**. After doing so, a confirmation page appears to regenerate the configurations for the devices with the selected Class of Service.

Deleting a Class of Service

You can delete any existing Class of Service, but before you attempt to do so, ensure that no devices are associated with that Class of Service. To delete a Class of Service, select the Class of Service for the specific device type that you want to delete and click **Delete**.

Tip When large numbers of devices associated with a Class of Service need to be deleted, use the Prime Cable Provisioning application programming interface (API) to write a program to iterate through these devices to reassign another Class of Service to the devices.

Note You cannot delete a Class of Service if it is designated as the default Class of Service or if devices are associated with it. Therefore, you cannot delete the **unprovisioned-docsis** Class of Service object.

Configuring Custom Properties

Custom properties let you specify additional customizable device information to be stored in the RDU database. To configure custom properties, click **Configuration > Custom Property**. Manage Custom Properties page is displayed, you use this page to add or delete custom properties.

Caution Although you can delete custom properties while they are currently in use, doing so could result in unexpected behavior.

To add a custom property, click **Add**. In addition to specifying the name and type of the property, you can also specify if the property needs to be encrypted (Check the **Encrypt Property** check box). This results in the property being available in the Property Encryption page also (see Property Encryption, on page 22).

After the custom property is defined, you can use it in the property hierarchy. See Property Hierarchy.

Configuring Defaults

You can access the default settings for the overall system, including the Regional Distribution Unit (RDU), Prime Network Registration extensions, and all supported technologies. To configure or view default settings, click **Configuration > Defaults.** The Configure Defaults page appears.

To access specific defaults page, click the specific link from the Default links on the left of the screen.

This section describes:

CableHome WAN Defaults

There are two distinct CableHome WAN default screens: one for WAN-Data devices and one for WAN-MAN devices. In either case, select the desired defaults from the list on the left pane.

- When you select the CH WAN-Data Defaults link, the CableHome WAN-Data Defaults page appears. Use this page to configure the WAN-Data device.
- When you select the CH WAN-MAN Defaults link, the CableHome WAN-MAN Defaults page appears. Use this page to configure the WAN-MAN device type.

Each WAN default page contains identical fields as described in the following table.

Table 1: Configure Defaults–CH WAN-Data/CH WAN-MAN Defaults Page

Field or Button	Description
CableHome WAN-Data Defaults/CableHome WAN-MAN Defaults	
Extension Point	Identifies the extension point to execute when generating a configuration for a WAN device.
Disruption Extension Point	Identifies the extension point to be executed to disrupt a WAN device.

Field or Button	Description
Service level Selection Extension Point	Identifies the extension used to determine the DHCP Criteria and Class of Service required for a device.
Default Class of Service	Identifies the current default Class of Service for a WAN-Data. New, unrecognized WAN devices are assigned to this Class of Service. Use the drop-down list to select a new default value.
Default DHCP Criteria	Identifies the current default DHCP Criteria for a specific device technology. New, unrecognized WAN devices are assigned this default DHCP Criteria. Use the drop-down list to select a new default value.
Automatic FQDN Generation	Automatically generates a host and domain name for the device. Two selectable options are available: • Enabled—Automatic generation of the FQDN is enabled. • Disabled—Automatic FQDN generation is disabled. **Note** See Automatic FQDN Generation , for additional information.
CableLabs Configuration Filename Script	Identifies the Groovy script to be used to generate the dynamic TFTP filename. **Note** This field appears only when you select the CableHome WAN MAN Defaults link.

Computer Defaults

When you select the Computer Defaults link, the list of default values currently applied to the computers supported by Prime Cable Provisioning appears. See Table 1: Configure Defaults–CH WAN-Data/CH WAN-MAN Defaults Page, on page 4 for the description of the fields that appear on this page.

Note Changes to the Default Class of Service or Default DHCP Criteria cause regeneration to occur. Other changes made to this page do not affect existing devices.

DOCSIS Defaults

When you select the DOCSIS Defaults link, the list of default values currently applied to the cable modems supported by Prime Cable Provisioning appears. The fields in this page are similar to the fields explained in Table 1: Configure Defaults–CH WAN-Data/CH WAN-MAN Defaults Page, on page 4. There are a few extra fields that appear in this page and those are explained in the following table.

Table 2: Configure Defaults–DOCSIS Defaults Page

Field or Button	Description
TFTP Modem Address Option	Identifies whether the TFTP modem address option is enabled.
TFTP Time Stamp Option	Identifies whether the TFTP server will issue a timestamp.
Note If you enable either or both of the TFTP options on this page, that appropriate TFTP information is included in the TFTP file before it is sent to the DOCSIS cable modem.	
CMTS Shared Secret	Identifies the character string that Prime Cable Provisioning uses in the calculation of the CMTS MIC in the configuration file. The CMTS uses it to authenticate the configuration file that a cable modem submits to the CMTS for authorization.
CMTS Default DOCSIS Version	Specifies the default DOCSIS version used by all CMTSs. If you do not enter a DOCSIS version in this field, it will default to version 1.0.
Relay Agent IP Address to CMTS Version Mapping file	Identifies the mapping file used by the CMTS. This file specifies the DOCSIS version that the CMTS will use.
Extended CMTS MIC Option	Identifies whether the Extended CMTS MIC (EMIC) option is enabled. **Note** Only if this field is enabled do subsequent fields in this section appears.
Extended CMTS MIC HMAC Type	Identifies the default Hash-based Message Authentication Code (HMAC) type for EMIC calculation. Choose one of the following HMAC type: • MD5 • MMH16 **Note** By default, MMH16 is used for EMIC calculation.
Extended CMTS MIC Digest Explicit Option	Identifies whether the Extended CMTS MIC Digest explicit digest option is enabled. By default, Extended CMTS MIC explicit digestion is used for EMIC calculation.
Extended CMTS MIC Shared Secret	Identifies the character string that Prime Cable Provisioning uses in the calculation of the Extended CMTS MIC in the configuration file. The CMTS uses it to authenticate the configuration file that a cable modem submits to the CMTS for authorization.
Dual-stack Mode	Enables or disables dual stack mode for all the DOCSIS devices.

Field or Button	Description
Dual-Stack Disruption Preference Mode	Identifies the preference of the IP address used for device disruption. This property is applicable only when Dual-Stack mode is enabled. By default dual-stack device disruption preference mode is set to *Dual-stack*. Choose one of the following device disruption preference modes: • IPv4—Uses IPv4 address to reset a device. • IPv6—Uses IPv6 address to reset a device. • Dual-stack—Uses both IPv4 and IPv6 address to reset a device.
IP Preference Mode	Identifies the IP preference value that can be set in the RDU. This value controls the type of IP address (IPv4 or IPv6), which is acquired by the eUE and which is used for Provisioning Flows. For details, see Configuring IP Preference Options.
Note The following fields can be used only for SNMPv3.	
DH Kick Start Reset Mode	Enables or disables the DH Kickstart mode.
DSS_ID Processing	Enables or disables the inclusion of DSS_ID while generating the DHCP instructions.

Note Changes to the default Class of Service or default DHCP Criteria cause regeneration to occur. Changes to any TFTP option come into effect starting from the next TFTP transfer.

Network Registrar Defaults

Prime Cable Provisioning provides Prime Network Registrar (NR) extension points that allow Prime Cable Provisioning to pull information from incoming DHCP packets to detect a device's technology. The extension points also let Prime Cable Provisioning respond to device DHCP requests with options that correspond to the configuration stored at the DPE.

When you select the NR Defaults link, the list of default values currently applied to Prime Network Registrar extensions appears. The following table identifies the fields that appear on this page.

Table 3: Configure Defaults–Network Registrar Defaults Page

Field or Button	Description
NR Extension Point Settings (Cisco BAC 4.0 and above)	

Field or Button	Description
Attributes Required in DHCPv4 Request Dictionary	Identifies a comma-separated list of attributes that the Network Registrar DHCPv4 request dictionary must include for Network Registrar extensions to submit a request to the RDU to generate a device configuration. The default value for this field is the relay agent remote ID option. If you do not set the **relay-agent-remote-id** value in this field, Network Registrar extensions reject devices from triggering a request for configuration generation.
Attributes from DHCPv4 Request Dictionary as Bytes	Identifies a comma-separated list of attributes pulled from the Network Registrar DHCPv4 request dictionary as bytes when sending a request to the RDU to generate a device configuration.
Attributes from DHCPv4 Request Dictionary as Strings	Identifies a comma-separated list of attributes pulled from the Network Registrar DHCPv4 request dictionary as strings when sending a request to the RDU to generate a device configuration.
Attributes Required in DHCPv6 Request Dictionary	Identifies a comma-separated list of attributes that the Network Registrar DHCPv6 request dictionary must include for Network Registrar extensions to submit a request to the RDU to generate a device configuration. The default value for this field is **none**.
Options Required in DHCPv6 Request Dictionary	Specifies a comma-separated list of DHCP options that the Network Registrar DHCPv6 request dictionary must include for Network Registrar extensions to submit a request to the RDU to generate a device configuration.
Attributes from DHCPv6 Request Dictionary as Bytes	Identifies a comma-separated list of attributes pulled from the Network Registrar DHCPv6 request dictionary as bytes when sending a request to the RDU to generate a device configuration.
Options from DHCPv6 Request Dictionary as Bytes	Specifies a comma-separated list of DHCP options pulled from the Network Registrar DHCPv6 request dictionary as bytes when sending a request to the RDU to generate a device configuration.
Attributes Required in DHCPv6 Relay Dictionary	Identifies a comma-separated list of attributes that the Network Registrar DHCPv6 relay dictionary must include for Network Registrar extensions to submit a request to the RDU to generate a device configuration. The default value for this field is **peer-address**.

Field or Button	Description
Options Required in DHCPv6 Relay Dictionary	Identifies a comma-separated list of DHCP options that the Network Registrar DHCPv6 relay dictionary must include for Network Registrar extensions to submit a request to the RDU to generate a device configuration.
Attributes from DHCPv6 Relay Dictionary as Bytes	Identifies a comma-separated list of attributes pulled out of the Network Registrar DHCPv6 relay dictionary as bytes for Network Registrar extensions to submit a request to the RDU to generate a device configuration.
Options from DHCPv6 Relay Dictionary as Bytes	Identifies a comma-separated list of DHCP options pulled out of the Network Registrar DHCPv6 relay dictionary as bytes for Network Registrar extensions to submit a request to the RDU to generate a device configuration.
NR Extension Point Environment Settings	
Attributes from Environment Dictionary	Identifies a comma-separated list of attributes pulled out of the Network Registrar environment dictionary as strings when sending a request to the RDU to generate a device configuration.

Note Changes made to this page do not take effect until the Prime Network Registrar extensions are reloaded.

PacketCable Defaults

The PacketCable Defaults page identifies those defaults necessary to support the PacketCable voice technology. When you select the PacketCable Defaults link, the list of default values currently applied to PacketCable devices appears. The fields in this page are similar to the fields explained in Table 1: Configure Defaults–CH WAN-Data/CH WAN-MAN Defaults Page, on page 4. There are a few extra fields that appear in this page and those are explained in the following table.

Table 4: Configure Defaults–PacketCable Defaults Page

Field or Button	Description
SNMP Set Timeout	Identifies the SNMP set timeout in seconds.

Field or Button	Description
MTA Provisioning Notification	Notification that an MTA event has taken place. An event occurs when the MTA sends its provisioning complete inform based on the selected choice. Options available include: • On Failure • On Success • During Provisioning • Always • Never
Dual-stack Mode	Enables or disables dual stack mode for all the PacketCable devices.
Dual-Stack Disruption Preference Mode	Identifies the preference of the IP address used for device disruption. This property is applicable only when Dual-Stack mode is enabled. By default dual-stack device disruption preference mode is set to *Dual-stack*. Choose one of the following device disruption preference modes: • IPv4—Uses IPv4 address to reset a device. • IPv6—Uses IPv6 address to reset a device. • Dual-stack—Uses both IPv4 and IPv6 address to reset a device.

RDU Defaults

When the RDU Defaults link is selected, the default settings that is configured for the RDU appear. Settings here can be changed accordingly to configure the RDU to communicate with Prime Network Registrar. For additional information, see the Cisco Prime Network Registrar End-User Guides.

The following table describes the fields that appear on the RDU Defaults page.

Table 5: Configure Defaults–RDU Defaults Page

Field or Button	Description
Configuration Extension Point	Identifies the common extension points executed before any other technology extension point is executed.
Device Detection Extension Point	Identifies the extension point used to determine a device type (for example, DOCSIS or computer) based on information pulled from the device DHCP Discover requests.

Field or Button	Description
Publishing Extension Point	Identifies the extension point to be used for an RDU publishing plug-in. This information is useful when you need to publish RDU data into another database.
Extension Point JAR File Search Order	Specifies the sequence in which the classes are searched in the JAR files that are listed in the preceding four fields.
Threshold Percentage for Regeneration Failure	Identifies the maximum acceptable percentage of failed devices. The acceptable values are 0.0 to 100.0%. By default this value is set to 0.0%.
Pause on Exceeding Failure Threshold	Identifies whether the Configuration Regeneration Service (CRS) is paused when the Threshold Percentage for Regeneration Failure is exceeded. There are two options: • Enable—Automatically pauses CRS when the Failure Threshold Percentage is exceeded. • Disable—CRS continues to regenerate configurations for rest of the devices. By default Pause on Exceeding Failure Threshold is enabled.
Scripts recompile	By default, script compilation mode is enabled and if enabled, the scripts get compiled and cached during file addition.
Number of Sessions per User	Specifies the maximum number of allowed sessions for a user. You could specify any value between 1 to 100. The default value for this property is 100. If this property value is not assigned to a user, the value available in the RDU defaults is considered.
Enable RADIUS Authentication	Identifies the authentication mode to be used. The options are: • Enable—Authenticates the user using the Radius server. • Disable—Authenticates the user in the local RDU database.

Configuration Details for Radius Authentication

The following table lists the fields required for configuring Radius authentication.

Table 6: Configure Defaults–RDU Defaults Page–Server Authentication Mode Property Details–RADIUS mode

Field or Button	Description
Primary Host	Identifies the primary IP address of the Radius server.
Primary SharedSecret	Identifies the primary shared secret used to authenticate the Radius server user.
Primary Port	Identifies the primary authentication port number of the Radius server. The default port number is 1812.
Secondary Host	Identifies the secondary IP address of the Radius server, which is optional.
Secondary SharedSecret	Identifies the secondary shared secret used to authenticate the Radius server user, which is optional.
Secondary Port	Identifies the secondary authentication port number of the Radius server, which is optional.
Timeout	Specifies the maximum length of time for which RDU waits for a response when trying to connect to the Radius server. The value will be specified in milliseconds and the default value is 1000 milliseconds. The value can be between 1000-5000 milliseconds.
Retries	Specifies the maximum number of times RDU attempts to connect with the Radius server. The default value is 1 and the value can be between 1-5.

Note If the Radius time out exceeds 10000 milliseconds then Prime Cable Provisioning authentication will fail. Radius time out and retries must be configured so that it does not exceed greater than 10000 milliseconds.

System Defaults

When you select the Systems Defaults link, the System Defaults page appears. The following table describes the fields that appear on this page.

Note The user can configure the default values using the Prime Cable Provisioning API.

Table 7: Configure System Defaults Page

Field or Button	Description
System Defaults	

Field or Button	Description
SNMP Write Community String	Identifies the default write community string for any device that may require SNMP information. The default write community string is private.
SNMP Read Community String	Identifies the default read community string for any device that can read or access the SNMP MIB. The default read community string is public.
Default Device Type for Device Detection	Identifies the default device type for a device not previously registered in the RDU. The options include: • DOCSIS • COMPUTER • PacketCableMTA • STB • CableHomeWanMan • CableHomeWanData • eRouter • RPD **Note** If the device detection extension is unable to identify the device type, the "default type" (for example, COMPUTER) specifies the device type. If you set the Default Device Type to None, the device record is not added to the RDU.
Maximum Diagnostics Device Count	Identifies the maximum number of MAC addresses (devices) that you can troubleshoot at any one time.
MIB List	Identifies a list of MIBs used by the RDU that do not require restarting the RDU.
Supplemental MIB List	Identifies an extended list of MIBs used by the RDU.
Excluded MIB Tokens	Defines those keywords, or tokens, that cannot be redefined by a MIB.
Excluded Supplemental MIB Tokens	Defines those additional keywords, or tokens, that cannot be redefined by a MIB and do not appear in the Excluded MIB Tokens list.
SNMP Defaults	

Field or Button	Description
SNMP Reset Version	Identifies the device SNMP reset version. The options include: • SNMPv1 • SNMPv2c • SNMPv3
SNMPv3 Security Name	Identifies the USM security name. The default value is docsisOperator when the DH Kickstart is enabled.
SNMPv3 Auth Protocol	Identifies the USM authentication protocol. The options are – 0 (NoAuth) / 1 (MD5) / 2(SHA). The default value is 1 (MD5) when the DH Kickstart is enabled.
SNMPv3 Priv Protocol	Identifies the USM privacy protocol. The options are – 0 (NoPriv) / 1 (DES) / 2 (AES). The default value is 1 (DES) when the DH Kickstart is enabled.
SNMPv3 Reset Security Mode	Identifies the USM security level. The options are - authPriv / authNoPriv / NoAuthNoPriv .
SNMPv3 Auth Key	Identifies the USM authentication key.
SNMPv3 Priv Key	Identifies the USM privacy key.
SNMPv3 Get Retries	Identifies the number of retires for *get* operation.
SNMPv3 Get Timeout	Identifies the timeout value for *get* operation.
SNMPv3 Set Retries	Identifies the number of retires for *set* operation.
SNMPv3 Set Timeout	Identifies the timeout value for *set* operation.
SNMPv3 Version Fallback Enabled	Enables or disables the SNMP version fallback.
Promiscuous Policy Settings	
CableHome WanData Promiscuous Mode	Enables or disables CableHome WAN-Data devices in the promiscuous mode.
CableHome WanMan Promiscuous Mode	Enables or disables CableHome WAN-MAN devices in the promiscuous mode.
Computer Promiscuous Mode	Enables or disables computers in the promiscuous mode.
PacketCable Promiscuous Mode	Enables or disables PacketCable devices in the promiscuous mode.
STB Promiscuous Mode	Enables or disables STBs in the promiscuous mode.

Field or Button	Description
eRouter Promiscuous Mode	Enables or disables eRouters in the promiscuous mode.
Promiscuous Mode For Devices Behind Unregistered CMs	Enables or Disables promiscuous access for devices behind unregistered Cable Modems.
CableHome WanData Promiscuous DHCP Criteria	Identifies the DHCP Criteria used to provision WAN-Data devices in the promiscuous mode.
CableHome WanMan Promiscuous DHCP Criteria	Identifies the DHCP Criteria used to provision WAN-MAN devices in the promiscuous mode.
Computer Promiscuous DHCP Criteria	Identifies the DHCP Criteria used to provision computers in the promiscuous mode.
Packetcable Promiscuous DHCP Criteria	Identifies the DHCP Criteria used to provision PacketCable devices in the promiscuous mode.
STB Promiscuous DHCP Criteria	Identifies the DHCP Criteria used to provision STBs in the promiscuous mode.
CableHome WanData Promiscuous Class of Service	Identifies the Class of Service used to provision WAN-Data devices in the promiscuous mode.
CableHome WanMan Promiscuous Class of Service	Identifies the Class of Service used to provision WAN-MAN devices in the promiscuous mode.
Computer Promiscuous Class of Service	Identifies the Class of Service used to provision computers in the promiscuous mode.
Packetcable Promiscuous Class of Service	Identifies the Class of Service used to provision PacketCable devices in the promiscuous mode.
STB Promiscuous Class of Service	Identifies the Class of Service used to provision STBs in the promiscuous mode.
CableLabs Configuration Filename Script	Identifies the Groovy script to be used to generate the dynamic TFTP filename.
eRouter Promiscuous DHCP Criteria	Identifies the DHCP Criteria used to provision eRouters in the promiscuous mode.
eRouter Promiscuous Class of Service	Identifies the Class of Service used to provision eRouters in the promiscuous mode.

STB Defaults

The STB Defaults page identifies those defaults necessary to support any STB compliant with CableLabs OpenCable Application Platform. This page contains identical fields as described in Table 1: Configure Defaults–CH WAN-Data/CH WAN-MAN Defaults Page, on page 4. There are a few extra fields that appear in this page and those are explained in the following table.

Table 8: Configure Defaults–STB Defaults Page

Field or Button	Description
Dual-stack Mode	Enables or disables dual stack mode for all STB devices.

Note Subsequent device configurations will include the changes you implement here. However, all existing configurations are not changed. To make the changes in any existing configuration, you must regenerate the configuration using the API.

eRouter Defaults

Table 9: Configure Defaults–eRouter Defaults Page

Field or Button	Description
Dual-stack Mode: enabled/disabled	Default value is disabled.
Dual-Stack Disruption Preference Mode: IPv4/IPv6/Dual-stack	Identifies the preference of the IP address used for device disruption. This property is applicable only when Dual-Stack mode is enabled in DOCSIS Defaults and eRouter Defaults. By default dual-stack device disruption preferencemode is set to Dual-stack. Choose one of the following device disruptionpreference modes: • • IPv4—Uses IPv4 address of the behind deviceto reset a device. • • IPv6—Uses IPv6 address of the behind deviceto reset a device. • • Dual-stack—Uses both IPv4 and IPv6 addressof the behind device to reset a device.

RPD Defaults

When you select the RPD Defaults link, the list of default values currently applied to the RPDs supported by Prime Cable Provisioning appears. See Table 1: Configure Defaults–CH WAN-Data/CH WAN-MAN Defaults Page, on page 4 for the description of the fields that appear on this page.

Note Changes to the Default Class of Service or Default DHCP Criteria cause regeneration to occur. Other changes made to this page do not affect existing devices.

Configuring DHCP Criteria

In Prime Cable Provisioning, DHCP Criteria describe the specific criteria for a device when selecting a scope in Prime Network Registrar. For example, a DHCP Criteria called **provisioned-docsis** has an inclusion selection tag called **tagProvisioned**. The DHCP Criteria is associated with a DOCSIS modem. When this

modem requests an IP address from the Prime Network Registrar, Prime Network Registrar looks for scopes associated with the scope-selection tag **tagProvisioned**.

To access the DHCP Criteria page, choose **Configuration > DHCP Criteria.** The Manage DHCP Criteria page appears, listing the DHCP Criteria that identify the technology DHCP Criteria that you have added.

Adding DHCP Criteria

To add a DHCP Criteria:

Step 1 From the Manage DHCP Criteria page, click **Add**.

Step 2 Enter the name of the DHCP Criteria you want to create.

Step 3 Enter the DHCP Criteria client-class name.

Step 4 Enter the inclusion and exclusion selection tags.

Note When creating new DHCP Criteria, the client-class and inclusion and exclusion selection tag names you enter must be the exact names from within Network Registrar. For additional information on client class and selection tags, see the Cisco Prime Network Registrar End-User Guides, and *CLIFrame.html* in the */docs* directory. You should specify either the client class, or inclusion and exclusion selection tag names, when creating a new DHCP Criteria.

Click **Assign Domain** and select the domain to which the property must belong. Click **Apply** to save the changes.

Note The options related to domain management and domain assignment are not enabled by default. For details, see Adding a Domain.

Step 5 To add a new property to the selected DHCP Criteria, click Add Property. Select the property from the drop-down and enter a value. Click **Save.**

Step 6 Click **Add.**

Step 7 Click **Submit.**

After the DHCP Criteria is successfully added in the RDU database, it will be visible in the Manage DHCP Criteria Page.

Modifying DHCP Criteria

Note Once you change the DHCP Criteria, subsequent device configurations will include the changes you implement. All existing configurations are regenerated, although the devices on the network will not get the new configuration until they are rebooted.

To modify existing DHCP Criteria, click the DHCP Criteria link that you want to modify. Make the desired changes to the client class, inclusion and exclusion selection tags, and the property value settings. Click **Submit.**

Deleting DHCP Criteria

Deleting DHCP Criteria using the administrator application does not delete the actual DHCP server configurations from the DHCP server. You must delete the DHCP server configurations manually.

To delete an existing criteria, select the DHCP Criteria you want to delete and click **Delete**.

Note You can delete a DHCP Criteria only if there are no devices associated with that criteria, and it is not designated as the default DHCP Criteria. If a DHCP Criteria has devices associated with it, you must associate a different DHCP Criteria before deleting the criteria.

Managing Files

Using the Prime Cable Provisioning Admin UI, you can manage the TFTP server files or template files for dynamic generation for DOCSIS, PacketCable MTAs, and WAN-MAN files, or software images for devices. Use this page to add, delete, replace, or export any file type, including:

- Template files—These are text files that contain DOCSIS, PacketCable, or CableHome options and values that, when used with a particular Class of Service, provide dynamic file generation.

  Note Template files can be created in any text editor, but must have a *.tmpl* file type. For additional template information, see Templates.

- Static configuration files—These files are used as a configuration file for a device. For example, a static configuration file, called *gold.cm*, would identify the gold DOCSIS Class of Service. Prime Cable Provisioning treats this file type like any other binary file.
- Firmware images—These are images of device firmware, which can be downloaded to devices to upgrade their functionality. Prime Cable Provisioning treats this file type like any other binary file. These firmware images can also include IOS images for Cisco devices.

The following table describes the fields that appear on the View Files page.

Table 10: View Files Page

Field or Button	Description

Search Type	Identifies the types of searches that you can perform for files using the Prime Cable Provisioning Admin UI. The options include:
	• Search by File Name—Searches for files using the filename pattern that you specify.
	• Search by File Type—Searches for files using the file type that you specify. The options include:
	  • Firmware File—Specifies a firmware image file.
	  • CableLabs Configuration File—Specifies a static configuration file for CableLabs.
	  • CableLabs Configuration Script—Specifies a configuration script file for CableLabs.
	  • CableLabs Configuration Template—Specifies a configuration template file for CableLabs.
	  • CableLabs Configuration Filename Script—Specifies a configuration filename with a script for CableLabs.
	  • Generic File—Specifies a generic file.
	  • JAR File—Specifies a JAR file.
	  • MIB File—Specifies a MIB file.

Search Criteria	Identifies the filename or file type. You can use an asterisk (*) as a wildcard character to search for partial filenames. For example, you can enter ***.cm** to list all files ending with the *.cm* extension. An example of an invalid wildcard is bronze*.
Files	Displays a list of files that match the search criteria. **Note** The check boxes immediately to the left of any selected item in this list must be checked before the item can be deleted.
View	Displays the details of the selected file.
File Type	Identifies the type of file.
Export	Exports any selected file to the client's computer.

Adding Files

To add an existing file:

Step 1 From the View Files page, click **Add**.

Step 2 Select the **File Type** from the drop-down list.

Step 3 Enter the path to the source file.

If you do not know the exact name of the source file, click **Browse** to navigate to the desired directory and select the file.

Step 4 Enter the name of the file.

If you are adding a CableLabs Configuration File or a Firmware File, you must also complete these steps, otherwise go to Step 6.

a) When adding a CableLabs Configuration File or a Firmware File, you can deliver the files that you add to the RDU to the DPE. To do so, click the **Enabled** radio button corresponding to the Is Deliverable field.

While Prime Cable Provisioning sets a deliverable status for each file type, you can change the default setting only for a CableLabs Config File or a Firmware File. The following list describes the default deliverable status for each file type:

- Firmware File—Enabled
- CableLabs Configuration File—Disabled
- CableLabs Configuration Template—Disabled
- Generic File—Disabled
- JAR File—Disabled
- MIB File—Disabled
- CableLabs Configuration Script—Disabled
- CableLabs Configuration File Name Script—Disabled

b) In the case of a Firmware File, additionally enter the file version and a suitable description for that version.

Step 5 Click **Assign Domain** and select the domain to which the file must belong. Click **Apply** to save the changes.

Step 6 Click **Submit**.

Note File sizes up to 4 MB are supported. If the size of the file that you are adding is over 4 MB, an error appears.

The View Files page appears, indicating that the file has been added.

Deleting Files

To delete an existing file, locate the file you want to delete using the search option. Choose the appropriate file or files and click **Delete.**

Caution Deleting a template file that is not directly linked to a Class of Service, but is referenced by another template/groovy file that is linked to a Class of Service, will cause the configuration regeneration service to fail.

Note You cannot delete a file that has a Class of Service associated with it. You must remove the Class of Service association before proceeding. See Configuring Class of Service, on page 1, for additional information.

Publishing Provisioning Data

Prime Cable Provisioning has the capability to publish the provisioning data it tracks to an external datastore in real time. To do this, a publishing plug-in must be developed to write the data to the desired datastore. The Manage Publishing page identifies information such as the plug-in name, its current status (whether it is enabled or disabled), and switch to enable or disable it.

You can enable as many plug-ins as required by your implementation, but remember that the use of publishing plug-ins can decrease system performance.

Note Prime Cable Provisioning does not ship with any publishing plug-ins. You must create your own plug-ins and load them into Prime Cable Provisioning in the same way as JAR files are (see Managing Files, on page 18). Then, manage the plug-ins from the Manage Publishing page.

Publishing Datastore Changes

To enable or disable a publishing plug-in:

Step 1 Choose **Configuration** > **Publishing** on the Primary Navigation bar.

Step 2 Click on the appropriate status indicator to enable or disable the required plug-in.

Note that as you click the status, it toggles between the two states.

Modifying Publishing Plug-In Settings

These settings are a convenient way for plug-in writers to store plug-in settings in the RDU for their respective datastore. To modify the publishing plug-in settings:

Step 1 Choose **Configuration** > **Publishing** on the Primary Navigation bar.

Step 2 Click the link corresponding to the plug-in you want to modify. The Modify Publishing Plug-Ins page appears.

The following table identifies the fields shown in the Modify Publishing Plug-Ins page.

Table 11: Modify Publishing Plug-Ins Page

Field	Description
Plug-In	Identifies the publishing plug-in name.
Server	Identifies the server name on which the datastore resides.
Port	Identifies the port number on which the datastore resides.
IP Address	Identifies the IP address of the server on which the datastore resides. This address is usually specified when the server name is not used.
User	Identifies the user to allow access to the data stored.
Password	Identifies the user's password, which allows access to the data stored.
Confirm Password	Confirms the password entered above.

Step 3 Enter the required values in the Server, Port, IP Address, User, Password, and Confirm Password fields. These are all required fields and you must supply this information before proceeding.

Step 4 Click **Submit** to make the changes to the selected plug-in.

Property Encryption

By default, the values assigned to custom properties and device properties at various entity levels like CoS, DHCP criteria and devices are stored as plain objects such as string, integer or boolean in the RDU. Considering this data to be sensitive, Prime Cable Provisioning lets you encrypt these properties. These property values are decrypted and returned as actual plain objects when you retrieve them using the API calls.

To enable property encryption:

Step 1 Choose **Configuration > Property Encryption** on the Primary Navigation bar.

The Property Encryption page lists all the encrypted properties, including encrypted custom properties. For details about encrypting custom properties, see Configuring Custom Properties, on page 3.

Step 2 You can also add a new property for encryption from the Property Encryption page. Click **Add Property**.

Step 3 Select the property to be encrypted and click **Save.**

Device properties can be added for encryption only through the Property Encryption page.

Note To disable encryption, select the properties from the Property Encryption list and click **Delete.**

Configuring CRS

Using the Prime Cable Provisioning Admin UI, you can manage the CRS requests more effectively. You use the Prime Cable Provisioning Admin UI to enable, disable, pause, and resume CRS. You can also view, filter, and delete any request queued by CRS. To manage these tasks you must be granted with the appropriate privileges. These management features are also available via RDU API.

The Manage Configuration Regeneration Service page, from the **Configuration** menu (**Configuration > CRS Management**), displays details and options to manage the CRS requests in the queue.

Click on the appropriate status indicator to enable, disable, pause and resume CRS. Note that as you click the status, it toggles between enabled and disabled, and running and paused states. You need not restart the RDU after changing any of the CRS states. By default, CRS is enabled.

- When CRS is in *Enabled* state, you can execute other CRS request management functionalities like, pause and resume CRS, view, filter, and delete any CRS request from the queue, and monitor CRS statistics.
- When CRS is in *Disabled* state, the entire CRS service is stopped and existing requests in the queue are cleared automatically. New regeneration requests is not posted in the CRS request queue.
- When CRS is in *Running* state, the CRS requests are executed starting from the top of the CRS queue and new requests are posted to the queue.
- When CRS is in *Paused* state, execution of CRS requests is paused. If CRS is paused during the execution of a batch, then CRS first completes execution of the current batch and then moves to the paused state. If any user creates a CRS request identical to a CRS request in the queue, it is replaced by the new CRS request. While in paused state, all new requests are posted to the existing CRS queue.

Viewing Request Policies and Status

The following table describes the policies set for CRS:

Table 12: CRS Policies and Status

Field	Description
Failure Threshold Percentage	Identifies the maximum acceptable percentage of failed devices per CRS request.
Pause on Exceeding Failure Threshold	Identifies whether CRS is set to pause when the failure threshold percentage is exceeded.
Pending Requests	Identifies the number of pending CRS requests to be executed.

Viewing Request Statistics

Statistics of the currently executing CRS request and the previous request are displayed in the Manage Configuration Regeneration Service page. Only when execution of a request is completed, the statistics related to it is displayed in the Previous Request tab. If a request is replaced by an identical request or is deleted during execution, it is not considered as a previous request.

The following table describes the statistics:

Table 13: CRS Statistics

Field	Description
State	Identifies the operational state of the configuration generation service. Some of the important CRS states are: • REGENERATION—Indicates that CRS is currently regenerating device configuration. • PAUSED—Indicates that CRS is paused. • DISABLED—Indicates that CRS is disabled.
Request ID	Identifies CRS request ID of the currently executing request.
Batch IDs	Identifies one or more batch IDs associated with a CRS request.
Search Type	Identifies the type operation that triggered the CRS request.
Device(s) Successfully Regenerated	Identifies the number of device configurations successfully regenerated for the currently executing request. **Note** The number of devices configuration regenerated may display more than the actual number of affected devices, since some devices are regenerated twice when: • CRS is paused during the execution of a CRS request and then resumed. • CRS is paused and paused request in the queue is replaced by identical CRS request.
Device(s) Attempted to be Regenerated	Identifies the total number of device configurations attempted to be regenerated for the currently executing request.
Elapsed Time	Identifies the time elapsed for the currently executing request, this does not include the paused time for request.
Regeneration Rate	Identifies the number of device configuration regenerated per second.
Device(s) Failed Regeneration	Identifies the number of devices that failed regeneration for a CRS request. The value is updated after completion of configuration regeneration of every 1000 devices of a request.
Percentage of Failed Devices	Identifies the running percentage of failed devices once the configuration regeneration of 1000 devices of a CRS request is completed. The status indicator indicates the device failure threshold level of the CRS request.

Note The CRS statistics is reset when RDU restarts, and when CRS is disabled and then enabled.

Viewing CRS Requests

CRS requests are queued in the order of creation on the Manage Configuration Regeneration Service pag page. A maximum of 1000 CRS requests are displayed in the Admin UI at a time. You can delete any or all of the CRS requests by selecting the requests you want to delete and click **Delete**. Use the quick filter and advanced filter options to search specific requests from the queue. These filter options search the CRS requests in the queue based on search type and username.

Note All external usernames are displayed as *External* in the Admin UI and *null* in the logs. External users cannot search CRS requests posted by any external user based on the username.

Privileges Required for CRS Operations

To view Manage Configuration Regeneration page and manage CRS operations from the Admin UI, you must be granted with the appropriate privileges.

Task	Privileges required
To enable CRS	PRIV_CRS_UPDATE and PRIV_PROP_UPDATE
To disable CRS	PRIV_CRS_DELETE and PRIV_PROP_UPDATE
To view the CRS status and statistics	PRIV_CRS_READ, PRIV_PROPERTY_READ, and PRIV_RDU_READ
To change the CRS settings Failure Threshold Percentage and Pause on Exceeding Failure Threshold from the RDU Defaults page	PRIV_PROPERTY_READ, PRIV_SYSDEF_READ, PRIV_SYSDEF_UPDATE, PRIV_USER_SECURITY, PRIV_CRS_UPDATE, PRIV_CRS_READ, PRIV_RDU_READ, PRIV_PROPERTY_UPDATE, PRIV_USER_UPDATE

To manage CRS operations from the APIs you must be granted with the appropriate privileges.

Task	Privileges required
To execute the command *IPDevice.regenConfigs()*	PRIV_CRS_CREATE
To set the properties *failureThresholdPercentage* and *pauseOnFailureThreshold*	PRIV_CRS_UPDATE and PRIV_PROP_UPDATE